



DEPARTMENT OF THE ARMY
HEADQUARTERS, U.S. ARMY ARMOR CENTER AND FORT KNOX
FORT KNOX, KENTUCKY 40121-5000

Expires 2 May 2007

REPLY TO
ATTENTION OF:

IMSE-KNX-IM (25)

2 May 2005

MEMORANDUM FOR

Commanders, All Units Reporting Directly to This Headquarters
Commanders, Fort Knox Partners in Excellence
Directors and Chiefs, Staff Offices/Departments, This Headquarters

SUBJECT: USAARMC Policy Memo No. 2-05 – Monitoring of Network Activity by the
Directorate of Information Management (DOIM)

1. References:

- a. AR 25-2, Information Assurance, 14 November 2003.
- b. AR 25-1, Army Knowledge Management and Information Technology Management, 30 June 2004.
- c. DODD 8500.1, 24 October 2002.
- d. DODI 8500.2, 6 February 2003.
- e. Fort Knox Reg 25-70, Procedures for the Entry of Information into the Fort Knox World Wide Web (WWW) Site/Internet and Use of Fort Knox Communications Resources, Appendix B, 12 April 2000.

2. The use of DOD and other government e-mail and computer systems (including the Internet) is limited to the conduct of official business or other authorized uses. Commanders and supervisors, at all levels, will educate employees on authorized and unauthorized uses of government computer systems.

3. All Fort Knox computer users must consent to monitoring of computer activity by clicking OK on the DOD banner before connection to the NIPRNET/INTERNET. They must read and sign the computer user guide (IASO responsibility to track). The DOIM employs devices/programs to monitor the network for unusual/inappropriate activity. Inappropriate activity is defined as any use of government computer systems in a way that would reflect adversely on DOD or the Army such as uses involving pornography or access to pornographic web sites; chain e-mail messages; unofficial advertising, soliciting or selling via e-mail; P2P (peer-to-peer); and other uses that are incompatible with public service. When activity is detected emanating

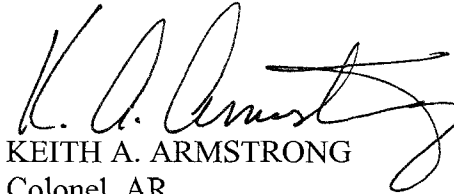
ATZK-IM (25)

SUBJECT: USAARMC Policy Memo No. 2-05 – Monitoring of Network Activity by the Directorate of Information Management (DOIM)

from a device, DOIM will contact the IASO/IMO, and the IASO/IMO will contact the supervisor. The IASO/IMO, with the supervisor's assistance, will research and provide necessary information to the Commander/Director of the organization so appropriate action can take place. It is the Commander/Director's responsibility to provide the Garrison Commander/DOIM, a report identifying the incident and measures taken to remedy the situation.

4. Point of contact is the DOIM Information Assurance Manager, 4-7201.

FOR THE COMMANDER:


KEITH A. ARMSTRONG
Colonel, AR
Garrison Commander